UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/593,124	11/22/2006	Olivier Charles	3340.231US01	9390

24113 7590 05/24/2010

PATTERSON THUENTE CHRISTENSEN PEDERSEN, P.A.
4800 IDS CENTER
80 SOUTH 8TH STREET
MINNEAPOLIS, MN 55402-2100

EXAMINER	
TOLENTINO, RODERICK	
ART UNIT	PAPER NUMBER
2439	

MAIL DATE	DELIVERY MODE
05/24/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/593,124	CHARLES ET AL.	
	Examiner	Art Unit	
	Roderick Tolentino	2439	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 September 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *19-37* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *19-37* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *0918/2006*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 19 – 37 are pending.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

2. The Specification of the instant application describes that the present invention can be implemented as software, thereby rendering the "means for" language in claim(s) 33 as computer software. *In re Donaldson Co.*, 16 F.3d 1189, 29 USPQ2d 1845 (Fed. Cir. 1994), decided that

> the "broadest reasonable interpretation" that an examiner may give means-plus-function language is that statutorily mandated in paragraph six. Accordingly, the PTO may not disregard the structure disclosed in the specification corresponding to such language when rendering a patentability determination.

See MPEP § 2181 also. Therefore, giving the claims their broadest reasonable interpretation, while keeping the structure disclosed in the specification in my mind, one of ordinary skill in the art would construe claim(s) 33 as representing a computer program *per se*.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and

the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 19 – 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Howard et al. U.S. Patent No. (6,519,647) in view of Duda U.S. Patent No. (5,708,710) and Aissi et al. U.S. PG-Publication No. (2005/0149730).

5. As per claim 19, Howard teaches transmitting an anonymous authentication request from a part of the client entity to the authentication entity (Howard, Col. 6 Lines 11 – 21, Anonymous authentication), transmitting the counter signature to the authentication entity (Howard, Col. 6 Lines 43 – 50, transmits signature), but fails to teach sending, from the authentication entity to the client entity, an authentication counter value corresponding to a current state of a counter of the authentication entity, verifying, at a client entity side, that the authentication counter value received is strictly greater than a counter value stored by the client entity, calculating, at the client entity side, a counter signature by applying a cryptographic function shared by the client entity and the authentication entity, wherein the authentication counter value and a secret key associated with the client entity are operands, updating the counter value stored by the client entity with the authentication counter value, searching, at an authentication entity side, for at least one identifiable client entity for which a corresponding counter signature for the authentication counter value is coherent with the counter signature received and increasing the authentication counter. However, in an analogous art Duda teaches sending, from the authentication entity to the client entity, an authentication counter value corresponding to a current state of a counter of the authentication entity (Duda, Col. 2 Lines 53 – 64, counter value), verifying, at a client entity side, that the

authentication counter value received is strictly greater than a counter value stored by the client entity (Duda, Col. 2 Lines 53 – 64, updating counter value), updating the counter value stored by the client entity with the authentication counter value (Duda, Col. 2 Lines 53 – 64, updating counter value), searching, at an authentication entity side, for at least one identifiable client entity for which a corresponding counter signature for the authentication counter value is coherent with the counter signature received (Duda, Col. 3 Lines 1 – 8, authenticating counter value) and increasing the authentication counter (Duda, Col. 2 Lines 53 – 64, updating counter value). And Aissi teaches calculating, at the client entity side, a counter signature by applying a cryptographic function shared by the client entity and the authentication entity, wherein the authentication counter value and a secret key associated with the client entity are operands (Aissi, Paragraph 0096, signature made with counter value and Key).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Duda's Method for authentication in communication system with Howard's method for synchronizing access control in a web server because it offers the advantage of reducing the amount of shared secret data (Duda, Col. 2 Lines 33 – 49).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Aissi's Multi-authentication for a computing device connecting to a network with Howard's method for synchronizing access control in a web server because it offers the advantage of avoiding connections to rogue access points (Aissi, Paragraph 0002).

6. As per claim 20, Howard as modified teaches wherein steps b) to h) are reiterated at least once to verify that the client entity identified is identical at each iteration (Howard, Col. 2 Lines 20 – 28, authenticating users).

7. As per claim 21, Howard as modified teaches the step of searching further comprises: calculating, for each identifiable client entity, the corresponding counter signature by applying the cryptographic function with the authentication counter value and the secret key associated with as operands to compile a list of identifiable client entities and corresponding counter signature couples, for the counter value (Duda, Col. 3 Lines 1 – 8, authenticating counter value) and verifying coherence between the counter signature received and at least one counter signature of the list (Howard, Col. 6 Lines 39 – 50, signature verifies user).

8. As per claim 22, Howard as modified teaches the list of identifiable client entities and corresponding counter signature couples compiled for a given authentication counter value is ordered, at the authentication entity side, according to the value of the counter signature Duda, Col. 3 Lines 1 – 8, authenticating counter value).

9. As per claim 23, Howard as modified teaches in a case of coherence between the counter signature received and the counter signature of a plurality of couples, steps b) to h) are reiterated until a single couple is obtained for which the counter signature corresponds to the counter signature received (Howard, Col. 6 Lines 39 – 50, signature verifies user).

10. As per claim 24, Howard as modified teaches, during reiteration of step i), the counter signature is calculated solely for the client entities corresponding to the plurality

of couples determined in the preceding iteration (Howard, Col. 6 Lines 39 – 50, signature verifies user).

11. As per claim 25, Howard as modified teaches implementing step i) as anticipated relative to an authentication request from a client entity at step a), wherein anticipated step i) comprises pre-establishing, at the authentication entity side, at least one authentication counter value to come, the list of identifiable client entities and corresponding counter signature couples for each of the authentication counter values to come (Duda, Col. 3 Lines 1 – 8, authenticating counter value), and storing the pre-established lists at the authentication entity side, wherein any sending from the authentication entity to the client entity of an authentication counter value corresponds to sending an authentication counter value for which a list of identifiable client entities and corresponding counter signature couples has already been pre-established (Duda, Col. 3 Lines 1 – 8, authenticating counter value).

12. As per claim 26, Howard as modified teaches step h) includes increasing the authentication counter by a fixed rate (Duda, Col. 2 Lines 53 – 64, updating counter value).

13. As per claim 27, Howard as modified teaches step h) includes increasing the authentication counter by a random rate (Duda, Col. 2 Lines 53 – 64, updating counter value).

14. As per claim 28, Howard as modified teaches in response to an authentication request, step b) comprises sending, at the authentication entity side and in addition to the authentication counter value, a random value associated with the counter value,

wherein the random value is different for each of the authentication counter values sent, and wherein each step of counter signature carried out during the method is replaced by a signature step of the authentication counter value and associated random value couple, including application of the cryptographic function further comprising the associated random value as operand (Duda, Col. 4 Lines 31 – 44, random number generator).

15. As per claim 29, Howard as modified teaches step c) includes verifying that the difference between the received authentication counter value and the stored counter value by the client entity is less than or equal to a predetermined value (Duda, Col. 3 Lines 1 – 8, threshold value).

16. As per claim 30, Howard as modified teaches, with step c) not being verified, the following intermediate steps are implemented: sending the counter value stored by the client entity from the client entity to the authentication entity; sending a temporary authentication counter value greater than the counter value stored by the client entity from the authentication entity to the client entity (Duda, Col. 2 Lines 53 – 64, updating counter value), then: implementing steps d) to g) on the basis of the temporary authentication counter value and, in the case of success of authentication of the client entity, updating the authentication counter value corresponding to the current state of the counter of the authentication entity with the temporary authentication counter value (Duda, Col. 3 Lines 1 – 8, authenticating counter value).

17. As per claim 31, Howard as modified teaches step e) includes transmitting the authentication counter value in addition to the authentication entity (Duda, Col. 3 Lines 1 – 8, authenticating counter value).

18. As per claim 32, Howard as modified teaches the authentication counter value is coded on at least 128 bits (Duda, Col. 2 Lines 53 – 64, counter value).

19. As per claim 33, Howard as modified teaches storing a secret key and executing the method of claim 19 (Howard, Col. 6 Lines 39 – 50, private key).

20. Claims 34 – 37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Howard et al. U.S. Patent No. (6,519,647), Duda U.S. Patent No. (5,708,710) and Aissi et al. U.S. PG-Publication No. (2005/0149730) and in view of Sakamura et al. U.S. PG-Publication No. (2004/0034766).

21. As per claim 34, Howard fails to teach a chip card. However, in an analogous art, Sakamura teaches a chip card (Sakamura, Paragraph 0043, IC Chips).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Sakamura's autonomous integrated-circuit card, with Howard's method for synchronizing access control in a web server because it offers the advantage of ensuring safe communication (Sakamura, Paragraph 0013).

22. As per claim 35, Howard as modified teaches the chip card comprises a contactless chip card (Sakamura, Paragraph 0043, Contactless mode).

23. As per claim 36, Howard as modified teaches a chip card reader including means for executing the method of claim 19 (Sakamura, Paragraph 0043, Card Reader).

As per claim 37, Howard as modified teaches the chip card reader comprises a contactless chip card reader (Sakamura, Paragraph 0043, Contactless mode).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Roderick Tolentino whose telephone number is (571) 272-2661. The examiner can normally be reached on Monday - Friday 9am to 5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Edan Orgad can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Roderick Tolentino
Examiner
Art Unit 2439

/R. T./

Examiner, Art Unit 2439

/Edan Orgad/
Supervisory Patent Examiner, Art Unit 2439